Naval Research Laboratory

Washington, DC 20375-5000

2

NRL Report 9178

On the Equation $X^a + Y^a = Z^a$

ALLEN R. MILLER

Industrial Engineering Services Branch
Engineering Services Division

February 7, 1989

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) NRL Report 9178	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Research Laboratory 6b OFFICE SYMBOL (If applicable) Code 2330	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code) Washington, DC 20375-5000	7b ADDRESS (City, State, and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

On the Equation $X^a + Y^a = Z^a$

12 PERSONAL AUTHOR(S)

Miller, Allen R.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
	FROM ____ TO ____	1989 February 7	11

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Fermat's last theorem Wright's generalized hypergeometric function

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The equation $X^a + Y^a = Z^a$ is solved for a as a function of X, Y, and Z in terms of a Wright function with negative unit argument. An equivalent form of Fermat's last theorem is given using this function.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL Allen R. Miller	22b TELEPHONE (Include Area Code) (202) 767-2215 22c OFFICE SYMBOL Code 2330

CONTENTS

ON THE EQUATION $X^a + Y^a = Z^a$

INTRODUCTION

In this report we study a problem related to Fermat's last theorem. Suppose that X, Y, and Z are positive numbers where

$$X^a + Y^a = Z^a. \tag{1}$$

We show that we can solve this equation for a; that is, we find a unique $a = a(X, Y, Z)$ in closed form. The method of solution is rather elementary, and we employ Wright's generalized hypergeometric function in one variable [1], as defined below:

$${}_p\Psi_q \left[\begin{matrix} (\alpha_1, A_1), \ldots, (\alpha_p, A_p); \\ \\ (\beta_1, B_1), \ldots, (\beta_q, B_q); \end{matrix} \; z \right] \equiv \sum_{n=0}^{\infty} \frac{\prod_{i=1}^{p} \Gamma(\alpha_i + A_i n)}{\prod_{i=1}^{q} \Gamma(\beta_i + B_i n)} \frac{z^n}{n!}.$$

When $p = q = 1$, we see that

$${}_1\Psi_1 \left[\begin{matrix} (\alpha, A); \\ \\ (\beta, B); \end{matrix} \; z \right] = \sum_{n=0}^{\infty} \frac{\Gamma(\alpha + An)}{\Gamma(\beta + Bn)} \frac{z^n}{n!}, \tag{2}$$

which is a generalization of the confluent hypergeometric function ${}_1F_1[\alpha; \beta; z]$.

AN EQUIVALENT FORM OF EQUATION (1)

In Eq. (1), the case $X = Y$ is not interesting since clearly

$$a = \frac{\ln(1/2)}{\ln(X/Z)}.$$

Therefore we shall assume without loss of generality that

$$Z > Y > X > 0,$$

and write Eq. (1) as

$$e^{a \ln(X/Z)} + e^{a \ln(Y/Z)} - 1 = 0.$$

Manuscript approved October 3, 1988.

Now making the transformation

$$e^{a\ln(Y/Z)} \equiv y, \tag{3}$$

we obtain

$$y^{\frac{\ln(X/Z)}{\ln(Y/Z)}} + y - 1 = 0,$$

and since

$$\frac{\ln(X/Z)}{\ln(Y/Z)} = \frac{\ln(Z/X)}{\ln(Z/Y)} > 1,$$

we arrive at

$$y^{\frac{\ln(Z/X)}{\ln(Z/Y)}} + y - 1 = 0. \tag{4}$$

Equation (4) is then equivalent to Eq. (1), and our aim is to solve this equation for y, thereby obtaining a. We note that it is not difficult to verify that Eq. (4) has a unique positive root y in the interval $(1/2, 1)$.

SOLUTION OF EQUATION (4)

In 1915, Mellin [2,3] investigated certain transform integrals named after him in connection with his study of the trinomial equation

$$y^N + xy^P - 1 = 0, \quad N > P, \tag{5}$$

where x is a real number and N, P are positive integers. Mellin showed that for appropriately bounded x, a positive root of Eq. (5) is given by

$$y = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(z)\, x^{-z} dz, \quad 0 < c < 1/P, \tag{6}$$

where

$$F(z) = \frac{\Gamma(z)\Gamma\left(\frac{1}{N} - \frac{P}{N}z\right)}{N\,\Gamma\left[1 + \frac{1}{N} + \left(1 - \frac{P}{N}\right)z\right]}$$

and

$$|x| < (P/N)^{-P/N}(1 - P/N)^{P/N-1} \le 2. \tag{7}$$

The inverse Mellin transform, Eq. (6), is evaluated by choosing an appropriate closed contour and using residue integration to find that

$$y = \frac{1}{N} \sum_{n=0}^{\infty} \frac{\Gamma\left(\frac{1}{N} + \frac{P}{N} n\right)}{\Gamma\left[1 + \frac{1}{N} + \left(\frac{P}{N} - 1\right) n\right]} \frac{(-x)^n}{n!}. \tag{8}$$

Under the condition shown in Eq. (7), Mellin, in fact, found all of the roots of Eq. (5). However, suppose we relax the restriction that N and P are positive integers. Instead, let N and P be positive numbers. We then observe that Eq. (8) gives *a fortiori* a positive root of Eq. (5) for positive numbers N and P. Further, without loss of generality we set $P = 1$, $N = \omega$. Then, using the Wright function defined by Eq. (2), we arrive at the following. The unique positive root of the transcendental equation

$$y^{\omega} + xy - 1 = 0, \quad \omega > 1, \tag{9}$$

where

$$|x| < \omega/(\omega - 1)^{1-1/\omega}$$

is given by

$$y = \frac{1}{\omega} \, {}_1\Psi_1 \left[\begin{matrix} \left(\frac{1}{\omega}, \frac{1}{\omega}\right) & ; \\ \left(\frac{1}{\omega} + 1, \frac{1}{\omega} - 1\right) & ; \end{matrix} \; -x \right]. \tag{10}$$

We observe that for any $|x| < \infty$, Eq. (9) has a unique positive root y. Equations (9) and (10) may also be obtained from Ref. 4, p. 713, Eq. (30).

Let us now apply the latter result to Eq. (4). On setting

$$x = 1$$

$$\omega^{-1} = \frac{\ln (Z/Y)}{\ln (Z/X)} \equiv \lambda,$$

and noting that $1 < \omega/(\omega - 1)^{1-1/\omega}$, we find

$$y = \lambda \, {}_1\Psi_1 \left[\begin{matrix} (\lambda, \lambda) & ; \\ (\lambda + 1, \lambda - 1) & ; \end{matrix} \; -1 \right], \quad 0 < \lambda < 1. \tag{11}$$

SOLUTION OF EQUATION (1)

We now solve Eq. (1) for a. From the transformation Eq. (3), we see that

$$a \ln (Y/Z) = \ln y. \tag{12}$$

Then, using Eq. (11), we arrive at the following. If $Z > Y > X > 0$ are such that

$$X^a + Y^a = Z^a ,$$

then

$$a = \frac{\ln \left\{ \lambda \, {}_1\Psi_1 \left[\begin{matrix} (\lambda, \lambda) & ; \\ (\lambda + 1, \lambda - 1) \, ; & -1 \end{matrix} \right] \right\}}{\ln (Y/Z)}, \tag{13}$$

where

$$\lambda \equiv \frac{\ln (Z/Y)}{\ln (Z/X)}, \quad 0 < \lambda < 1. \tag{14}$$

We now prove the following. Consider for $X < Y$, $M \geq 1$, the diophantine equation

$$X^M + Y^M = Z^M.$$

Then the positive integers X, Y, and Z must satisfy

$$X^\lambda Y^{-1} Z^{1-\lambda} = 1 , \tag{15}$$

where λ is an irrational number such that $0 < \lambda < 1$.

From Eq. (12) we have

$$(Y/Z)^M = y, \tag{16}$$

so that y is a rational number in the interval $1/2 < y < 1$, as we noted earlier. If λ is rational, there exist relatively prime integers s and t such that

$$\lambda = \omega^{-1} = s/t.$$

Hence, y is the unique positive root of

$$y^{t/s} + y - 1 = 0.$$

Now since $\lambda < 1$, then $s < t$, and we obtain the polynomial equation of degree t with integer coefficients:

$$y^t + (-1)^s y^s + \ldots + 1 = 0.$$

The only positive rational root that this equation may have is $y = 1$ [5, p. 67]. But $y < 1$, so the assumption that λ is rational leads to a contradiction. We have then that λ is irrational, and Eq. (15) follows from Eq. (14). This proves our result. Another proof of this result [6] is given in the appendix of this report.

The Wright function ${}_1\Psi_1$ appearing in Eq. (13) depends only on the parameter λ. Thus, for brevity, we define

$$\Psi(\lambda) \equiv {}_1\Psi_1 \left[\begin{matrix} (\lambda, \lambda) & ; \\ (\lambda + 1, \lambda - 1) \; ; & -1 \end{matrix} \right], \quad 0 < \lambda < 1.$$

From our previous result, we see that if Fermat's theorem* is false, then there exist positive integers $X < Y < Z$ such that λ is irrational.

Therefore, Fermat's theorem is false if and only if there exist positive integers $Y < Z$, $M > 2$ and an irrational number λ $(0 < \lambda < 1)$ such that

$$(Y/Z)^M = \lambda\Psi(\lambda).$$

Thus Fermat's conjecture may be posed as a problem involving the special function $\lambda\Psi(\lambda)$. We remark that recently, Fermat's conjecture has been given in combinatorial form [7].

SOME ELEMENTARY PROPERTIES OF $\lambda\Psi(\lambda)$

The series representation Eq. (17) for $\lambda\Psi(\lambda)$ does not converge for $\lambda = 0, 1$. Nevertheless, it is natural to define

$$\lambda\Psi(\lambda)\Big|_{\lambda=1} = 1/2, \quad \lambda\Psi(\lambda)\Big|_{\lambda=0} = 1.$$

Below we give a brief table of values for $\lambda\Psi(\lambda)$ correct to five significant figures:

λ	$\lambda\Psi(\lambda)$	λ	$\lambda\Psi(\lambda)$
0.0	1.00000	0.6	0.58768
0.1	0.83508	0.7	0.56152
0.2	0.75488	0.8	0.53860
0.3	0.69814	0.9	0.51825
0.4	0.65404	1.0	0.50000
0.5	0.61803		

Observe that we may write the inverse relation

$$\lambda = \ln \lambda\Psi(\lambda)/\ln [1 - \lambda\Psi(\lambda)].$$

*Fermat's theorem states that there are no integers $x, y, z > 0$, $n > 2$ such that $x^n + y^n = z^n$.

The following series representations for $\lambda\Psi(\lambda)$, $0 < \lambda < 1$ may easily be derived from the first one below:

$$\lambda\, {}_1\Psi_1\left[\begin{matrix}(\lambda, \lambda) & ; \\ (\lambda + 1, \lambda - 1) ; \end{matrix} \; -1\right] = \lambda \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \frac{\Gamma(\lambda + \lambda n)}{\Gamma(\lambda + 1 + (\lambda - 1)n)} \tag{17}$$

$$= \frac{\lambda}{\pi} \sum_{n=1}^{\infty} \frac{(-1)^n}{(1 - \lambda)n - 1} \sin[\pi(1 - \lambda)n]\, B(\lambda n, n - \lambda n) \tag{18}$$

$$= 1 - \lambda \sum_{n=0}^{\infty} (-1)^n \, {}_2F_1[-n, (1 - \lambda)(n + 2); 2; 1] \tag{19}$$

$$= 1 + \lambda \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \binom{\lambda(1 + n) - 1}{n - 1} . \tag{20}$$

Equation (18) follows from Eq. (17) by using $\Gamma(z)\Gamma(-z) = -\pi/z \sin \pi z$; $B(x, y)$ is the beta function. Equation (19) follows from Eq. (17) by using Gauss's theorem for ${}_2F_1[a, b; c; 1]$. And Eq. (20) follows from Eq. (17) by using $\binom{\alpha}{m} = \Gamma(1 + \alpha)/m!\,\Gamma(1 + \alpha - m)$. Equation (20) for $1/\lambda$, an integer greater than one, is due to Lagrange [2, p. 56].

CONCLUSION

The equation $X^a + Y^a = Z^a$ has been solved for a as a function of X, Y, and Z in terms of a Wright function ${}_1\Psi_1$ with negative unit argument. An equivalent form of Fermat's last theorem has been given using this function. Further, some elementary properties of ${}_1\Psi_1$ have been stated.

REFERENCES

1. H.M. Srivastava and H.L. Manocha, *A Treatise on Generating Functions* (Halsted Press, 1984).

2. M.G. Belardinelli, "Résolution Analytique des Equations Algebraiques Generales," *Mémorial des Sciences Mathematiques*, Fascicule 145 (Gauthiers-Villars, 1960).

3. H. Hochstadt, *The Functions of Mathematical Physics* (Wiley, 1971).

4. A.P. Prudnikov, Yu. A. Brychkov, and O.I. Marichev, *Integrals and Series*, Vol. 1 (Gordon and Breach, 1986).

5. S. Borofsky, *Elementary Theory of Equations* (MacMillan, 1950).

6. W.P. Wardlaw, unpublished communication, July 1988.

7. W.V. Quine, "Fermat's Last Theorem in Combinatorial Form," Amer. Math. Monthly, **95**, 1988, p. 636.

Appendix

Theorem: Consider for $X < Y$, $M \geq 1$, the diophantine equation

$$X^M + Y^M = Z^M. \tag{A1}$$

Then the positive integers X, Y, and Z must satisfy

$$X^{\lambda} Y^{-1} Z^{1-\lambda} = 1, \tag{A2}$$

where λ is an irrational number such that $0 < \lambda < 1$.

Proof: Clearly $0 < X < Z$ and $0 < Y < Z$. Define $f(\lambda) \equiv (X/Z)^{\lambda}$ which is a decreasing continuous function of λ on $[0, 1]$, since $(X/Z) < 1$. Since $f(0) = 1$, and $f(1) = X/Z$, by the intermediate value theorem there is a λ in the interval $(0, 1)$ such that

$$f(\lambda) = \left(\frac{X}{Z}\right)^{\lambda} = \frac{Y}{Z} \tag{A3}$$

if and only if

$$\frac{X}{Z} < \frac{Y}{Z} < 1.$$

We know $Y/Z < 1$, so such a λ exists if and only if $X < Y$. Hence Eq. (A3) implies Eq. (A2).

To show λ is irrational, suppose p is a prime dividing X and Y. Then Eq. (A1) implies p divides Z. Similarly, if p divides any two of X, Y, or Z, it divides all three, and p^k must divide all three with the same maximum exponent k. Since $X < Y$, there must be some p^k that divides Y but does not divide X. Hence, p^k also does not divide Z. Suppose $\lambda = a/b$ is rational where a and b are relatively prime. Then by Eq. (A3)

$$\left(\frac{X}{Z}\right)^{a/b} = \frac{Y}{Z}$$

which implies

$$X^a Z^b = Y^b Z^a. \tag{A4}$$

Since p^k divides Y, it divides the right side of Eq. (A4). But p^k not dividing X or Z implies p^k does not divide the left side of Eq. (A4), and we have a contradiction. Thus λ must be irrational.

END
FILMED
5-89
DTIC